Copy sent HQSG 8/3
Signals 5.

15(T)

TOP SECRET

TICOM/I-192

REPORT BY DR. REGULA ON GERMAN METEOROLOGICAL CYPHER SYSTEMS AND THE GERMAN MET. INTELLIGENCE SERVICE

The attached report was written in December, 1945, by a Dr. REGULA at the request of F/Lt. SNIDER formerly of R.A.F. "Y", and received from G.S.I.(s), H.Q., British Army of the Rhine under reference BAOR/IS/INT/101/118 dated 8th February, 1946.

2. The report is in sections:-

A. The Cypher Systems of Germany and Allied Countries
B. Organisation of the German Meteorological Intelligence Service.
C. Foreign Meteorological Intelligence and Cypher Systems.
D. Cypher Machines
E. Miscellaneous

TICOM

2nd March, 1946.

No. of Pages. ~~12~~ 13

Distribution

British

D.D.I
H.C.G.
D.D.(M.F.)
D.D.(A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (4) (via Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, A.S.A. Europe
Col. Kunkel, USAFE.

TICOM

S.A.C. (3)
Cdr. Manson
Capt. Collins
Ticom Files (4)

Additional

S.A.C. for Signals 5, Air Ministry.

Dr. Walter Regula
(22) Wuppertal-Elberfeld
Kronprinzenallee 97

Wuppertal
26 December 1945.

F/Lt. D.F. Sander
Room 64
GS I
HQ I Corps District
B.A.O.R.

Dear Mr. Sander,

I send you herewith the desired report on "Cryptanalysis and the Wireless Intercept Service". It contains 12 pages and a further supplement.

I willingly put myself at your service for further and more detailed information on all cryptanalytical and similar matters.

Yours respectfully

(signed) Dr. Regula

Cryptanalysis and Wireless Intercept Service.

A) The Cypher systems of Germany and Allied Countries

1) Auka Tables
2) Aircraft safety traffic
3) Weather substitution tables
4) Special "S" substitution tables
5) Special weather substitution tables
6) Hand keys
7) Weather machine key "East"
8) Hungarian weather summaries
9) Wireless advice service
10) 'Zenit' code
11) 'Astra' figures

B) Organization of the German Meteorological Intelligence Service

1) Specialists
2) Wenüb
3) Cooperation
4) Teleprinter network 'East'
5) Cypher teleprinters

C) Foreign Meteorological Intelligence and cypher systems

1) European Russia
2) Canada - U.S.A. - Asiatic Russia
3) Azores
4) England
5) 'Westa' Reports
6) 'Fasan' Reports
7) 'Widder' Reports
8) Russian cypher systems
9) Turkish cypher systems

D) Cypher machines

1) Enigma
2) Machine for weather reports

E) Miscellaneous

Cryptanalysis and Wireless Intercept Service

A. The cypher systems of Germany and allied countries.

1) Auka Tables.

Battle, location and S.O.S. reports also reconnaissance reports were sent in figures with the Auka tables. These figures were encyphered by the aircraft observor with a cypher sheet, size roughly 10 x 15 cm. This cypher sheet was printed on both sides, it included the figures from 0 to 999 and the heading was in German and Italian. The sheets were made up into books each of 31 sheets. A fresh sheet was valid each day.

2) Aircraft Safety Traffic

At the beginning of the war the aircraft safety traffic was carried out normally, i.e. as in peace-time. In the subsequent course of the war, owing to enemy interception of German wireless traffic, it was ordered that, with regard to weather reports, aircraft might only request two Q groups from the D/F station, for instance QFE and QAN or QBB and QFF etc. By this means the enemy was to be prevented from obtaining complete German weather reports. Later on special cypher strips for the aircraft safety traffic were issued to aircraft wireless operators for reporting flights to the aircraft control. Details of this cypher system are not known.

3) Weather Substitution Tables

a) Cypher Systems

From the beginning until the end of the war, weather reports, which were encoded with the international code, were recyphered. At the beginning of the war a five element group:- ..... xxxxx ..... was divided into two groups each of two or three figures and these were recyphered with the G.A.F. weather substituion tables as three or two digit figures. The cypher sheet was changed every three hours. The calendar, by which the change took place, was given at the beginning of the book. The unencyphered reports were entered in red transmission books and the encyphered ones in white books.

Disadvantages It frequently happened, owing to carelessness by personnel, that unencyphered reports got into possession of the wireless operator and were sent out by him. In order to set an easy standard for the transmission of reports by wireless operators not used to the weather code, a new system was introduced in the first half of the war. The five digit group

..... xxxxx .....

was split into two three-digit figures

..... xxa bxx .....

so that a + b gave the middle figure. Tens which might appear in decypherment were omitted.

These two three-digit groups were encyphered as three-digit groups in the weather substitution tables. The encyphered report then appeared as

..... yyyyyy .....

b) The arrangement of the substitution tables.

Encyphered and decyphered figures in the tables were not connected with each other by any regularity. The juxta-position of the figures was a matter of change, figures were drawn at random from a hat and put into a printers compositors box by the side of the unencyphered figures.

c) Advantages

Decypherment was impossible without the substitution tables.

d) Disadvantages

The tables presented a confusing mass of figures. Only after lengthy practice could the codist find the figure required immediately and without a considerable loss of time.

4) Special "S" substitution tables (Siegfried)

From 1943 the weather reports of Rumania and a few other allied countries were encoded by the same method as in the Reich (see (A 3). As a precaution against espionage they were not, however, encyphered with the weather substitution tables in use in the Reich but with special, so-called "Siegfried Tables" Until 1943 another cypher system, the so-called "Adder [Wurm] System" was used in Rumania, Bulgaria and Hungary. The encyphered messages were continuous, i.e., the individual weather reports were not separated from each other by breaks. Under the individual figures were written other figures taken from certain tables, which were different for Rumania, Bulgaria and Hungary and these were subtracted from the other ones, i.e. from the encyphered messages received by wireless. The system was generally considered to be inconvenient and for this reason it was replaced by the "S" substitution table system.

5) Special weather substitution tables

Only a very few copies were available with the chief meteorological stations operating with the operational HQ. The serial numbers of the individual tables were correspondingly very low. As a distinctive feature these red tables had a broad green band diagonally from the bottom left to the upper right corner on the front. Weather reports from the fighting area were encyphered with these substitution tables in accordance with the method, described above, of converting five-digit groups into six digit groups, (see paras C 6 and 8, D2). The system was valid from about January 1943 to January 1945.

6) Hand Key

During the first years of the war, also in Russia in the early days, the so-called hand-key for the encypherment of weather reports was in use. The reason for its introduction was that during quick advances the Meteorological Trupps in the most forward lines could not be supplied with new cypher data in time, should a change of substitution tables be carried out. These operationally important weather reports might thus be lost. The hand-key, therefore, comprised a more simple cypher system with no printed data. I do not know in detail by which system encypherment was carried out. In the course of the war this method was made obsolete.

7) Weather Machine Key "East"

During the campaign in the East a separate machine key "East" was in use for the East and for the Meteorological Service. Its purpose was the encypherment of weather summories, command wireless and the instructions for change of substitution tables. Encypherment was effected by the "Enigma" cypher machine, in general use.

8) Hungarian Weather Summaries (See Appendix A)

With the occupation of Hungary by German troops in 1943/1944, a new cypher system for the dissemination of weather summaries was introduced by Komm Ung (G.O.C. Hungary). This system developed from the fact that only a limited vocabulary is necessary for weather summaries within a certain area. This vocabulary, together with a table of letters and figures, was put in a rectangle. The individual terms were contained within this rectangle according to geographical and meteorological groups but in irregular order. The vocabulary was modified in January 1945. The abcissae and ordinates of the rectangle were provided with cypher strips, they were changeable and were changed after roughly 3 or 4 months. To encypher a word three letters were therefore necessary, for example

Hudapest Rain = LMA LEB

Advantages: The merits of this system were in the simplicity of the cypher material.

Disadvantages: The disadvantages were that it was not absolutely secure and that yet another method was applicable to the weather summaries encyphered by the "enigma".

9) Wireless Advice Service

In 1943 in the Crimea a wireless advice service was instituted for the first time, in order to economize in personnel. Its task was to issue by wireless to all the smaller airfields in the Crimea not having meteorologists, weather advice reports prepared by a central station for the use of courier and transport aircraft. Here also, a certain vocabulary was available which, like 8, was encyphered by letters.

Example.

CFA	Sector	Sarabus	- Saki
DBJ	"	"	- Kertsch
MZC	"	"	- Odessa
OTR	"	"	- Constanza
NHB	"	Saki	- Odessa
HCF	"	"	- Constanza
JSQ	"	Kertsch	- Saki
LPG	"	"	- Dniepropetrowsk
JKY	"	"	- Zaporoshe

etc.

SVZ	Qbb
UVA	Qbj
WOL	Qba
PST	falling

etc.

I do not know whether encypherment was carried out in three or five digit groups. The method was put into effect and was introduced, in the winter of 1944/45 into all the areas controlled by Germany. Certain modifications were necessary for the requirements of the various larger areas the vocabulary had to be larger. Encypherment was, moreover, effected with the figures from 0 to 999.

Advantages: Considerable personnel economy

Disadvantages: Mechanization and incompleteness of the weather advice.

10) "Zenit" Code

The Zenit code and its encypherment may be known. At the beginning of the war reports prepared from the Zenit code were sent by wireless unencyphered. In the further course of the war the figures (location groups) were first encyphered, later the letter groups also, with a special cypher strip which had a 4-letter indicator at the top. Towards the end of the war the figures were also encyphered with this cypher strip. A special strip was used for each flight; it was made known to the receiver by the indicator at the beginning of the report.

11) "Astra" figures

Various weather observations which could not be expressed with the "Zenit" code were encoded and encyphered at the end of a Zenit report as Astra figures - that is within the framework of the Auka tables (see A1). For instance: cloud becoming lower in direction .....Astra figure: 32

B. Organisation of the German Meteorological Intelligence Service

1) Specialists

Oberregierungsrat Wüsthoff was a specialist in the Meteorological Intelligence Service. Oberst Birnbaum (?) was allotted to him as liaison officer to represent matters of the Meteorological Service at the G.A.F. signals troop and to put all the measures into effect.

2) Wenüb

The Meteorological Intelligence Control [Wetternachrichtenüberwachung - Wenüb] was located in Berlin Glindow. Their task was the wireless monitoring of all meteorological transmitters including those of the enemy.

3) Co-operation

With the individual Luftflotten the meteorological service and G.A.F. Signals units (Gr LMS) worked in close co-operation. By this means the evaluation of foreign signals material was ensured. Only after some time, did this co-operation work smoothly. In the Balkans campaign, as well as at the beginning of the Russian campaign, the meteorological service suffered from a lack of signals communications owing to technical difficulties which were particularly great in these countries. Only in the subsequent course of the Russian war did signals communications function perfectly.

4) Teleprinter Network "East"

As in the Reich, unencyphered weather reports were circulated not only by wireless but also by teleprinter broadcast and also in the occupied Russian areas. A separate broadcast teleprinter network "East" was introduced. The meteorological stations at Lwow, Kiev and Zaporoshe were included amongst those in the broadcast teleprinter network "East".
Advantages: no encypherment
Disadvantages: technical shortcomings; liable to be tapped.

5) Cypher Teleprinters

In allied countries weather reports were circulated by means of the "cypher teleprinter" owing to danger of espionage. The meteorological station at Bucharest - Baneasa was included amongst those possessing a "cypher teleprinter"

C. Foreign Meteorological Intelligence and Cypher methods.

1) Russia

In the winter of 1939/1940 when Germany stopped the circulation of P/L weather reports owing to the war and Russia, in the Finnish-Russian War, did the same a number of German weather reports were, by arrangement, exchanged several times daily (about 10) for reports from European Russia. As it transpired, Russia betrayed these highly confidential reports to the western enemies of Germany; the exchange of reports was, thereupon, stopped.

2) Canada - U.S.A. - Asiatic Russia

Because they were not encyphered, reports from Canada, U.S.A. and Asiatic Russia were available at the beginning of the war. Indirectly, they were of great use to German meteorology.

3) The Azores

The weather reports of the Azores, which were so important for weather forecasts for the British Isles and France, were received unencyphered in Germany for months after occupation by the Allies. This was apparently an oversight on the part of the enemy intelligence service.

4) England

Weather reports from England could periodically be decyphered. Even in periods when this was not possible, numerous QFE's of English places were available.

5) Westa Reports

The German and foreign intelligence material was supplemented by numerous flights by the weather reconnaissance squadrons using the "Zenit" code (see A 10). Weather reports which were transmitted continuously from the aircraft whilst over enemy territory at first, were later accumulated owing to increasing enemy defence and sent out during the return flight over friendly territory.

6) "Fasan" reports

Especially secret weather reports from enemy territory were passed by telephone, under the cover name "Fasan", by Berlin to the Control Meteorological Stations immediately concerned. The weather reports were not encyphered except for the station indicator. Those "Fasan" reports which were sent out by means of the above mentioned broadcasts were encyphered on the special weather substitution tables.

7) "Widder" reports

In order to inform the participating meteorological stations of the position of the encyphered stations indicated under C 6, "Widder" reports were sent at the same time by telephone to the meteorological stations concerned. They consisted of two five-element groups, after the code word "Widder", which gave the indicator of the "Fasan" report and the geographical position of the stations listed in it.

8) Russian Cypher System

a) Aerological reports

Even at the beginning of the war when Russian weather reports were already encyphered it was always possible to decypher the Russian aerological reports. One or two days were necessary to discover the key but this was always worthwhile since the Russians only changed the key about every three weeks.

b) Russian Cypher System

In the subsequent course of the war the decyphering of Russian reports was better organized. Germany possessed the original Russian cypher tables.

The Russian cypher system consisted, like the old Rumanian, of an adder system. The subtractor/adder was sent out by wireless once daily and this was used in conjunction with the Russian cypher tables to decypher the Russian reports. This work was generally done centrally in Berlin for all the units concerned. The Russian reports thus decyphered were re-encyphered by the Special Weather Substitution Table (see A 5) and broadcast by the transmitter with the call-sign LPK twice daily. The weather reports at 0800 and 1900 hours which were broadcast in the period from 1145 to 1200 hours and from 2345 to 2400 hours are referred to here. There were, therefore, 4 or 5 hours between the weather observation in Russia, the encypherment and transmission of the report there and the German decypherment and re-encypherment of it. By this method the German meteorological service often had 120 reports from enemy occupied European Russia in every observation period. In time the quality of the Russian reports deteriorated and this led one to believe that the Russians knew the Germans were reading their reports and intentionally included bogus reports for the purpose of deception. Towards the end of the war the amount of Russian observation material also left much to be desired. Numerous reports were available from the Moscow area and the Urals district; other areas appeared less and less frequently in the reports. From the distribution of weather reports it was concluded that the Russian Meteorological Organisation could not keep pace with the advance of the troops. Between the front and the area covered by reports from transmitter LPK was a blind area more than 100 kms wide. An improvement of this state of affairs was apparent for the first time during the fighting in Hungary.

c) By means of the interception of the Russian aircraft safety service in Hungary, Germany came into possession of numerous weather reports from the immediate area of the Russian front. It was, moreover, plain that the Russians were endeavouring to organize the meteorological service in the area of the front more efficiently. They did not use the cypher system in use in Russia. The cypher system used in this area is not known. It was, presumably, comparable to the German hand-key (see A 6). In any case the key could not have been complicated since comparatively inexperienced personnel decyphered it.

d) Agents Reports

Additional weather reports from Russian occupied territory were organized by the Germans. They were sent by wireless several times daily by parachutist agents who were dropped far behind the enemy front. The German meteorological service received them in the following form:

GGXXX YYYC_1C_m WW... .....

GG = time, XXX = longitude, YYY = latitude, the remaining symbols as in the international code. It is doubtful whether these reports were sent by wireless in this form to the receiving station which "vetted" them for the meteorological station.

The school, which trained these parachutist agents, occasionally sent out practice weather reports which consisted of two five-element groups (-LG... .....) in which the day of the week L, the time G, observation, cloud base, visibility, cloud cover, direction and strength of wind as well as the observation station were given. This key also was very secret.

e) There was no evidence that the Russians were in possession of German weather reports from the East Front. It is also doubtful whether they seriously intended to investigate them. Russian military operations were faultlessly based on many years experience of climatic and weather conditions (it is thought) so that they did not need the current synoptics.

d9) Turkish Cypher Systems

In 1941/1942 it was possible to break the Turkish weather code on several occasions. It merely consisted of the transposition and splitting up of the code symbols of the international code. Later on, however, it became increasingly difficult to break and it was one of the most difficult problems for the German intelligence service. Only towards the end of the war could Turkish weather reports again be regularly circulated by station LPK but shortcomings in the quality led one to conclude that the Turkish reports were not being completely decyphered.

By reason of the outstandingly efficient German Meteorological Intelligence Service the situation in the winter of 1942/43 was such that Germany was in possession of almost all the European and many non-European secret weather reports. The number of weather reports was, moreover, larger than in peace-time.

D) Cypher Machines

1) Enigma

To encode texts the "Enigma" machine which is presumably known, was generally used. The wheels of the machine had, for the day in question, positions fixed in relation to each other and to the casing. The indicator group of the report to be encyphered was then "typed" on the key-board and this gave the final wheel position. When this was adjusted the machine was ready to encode the wireless message.

2) Machine for weather reports

Towards the end of the war, i.e. in January 1945, the encypherment and decypherment of weather reports from enemy territory, which had hitherto been done with the Special Weather Substitution Table (see A5 and C8), was carried out with a code machine for figures. There were only a very few models available and it more or less corresponded to the "Enigma" machine. The individual figures were 'typed' on a keyboard, and the encyphered and plain-language report thereupon appeared on two different strips of paper.

The technical performance of the machine was not perfect and it repeatedly suffered from mechanical defects.

E) Miscellaneous

1) At the beginning of the war the weather reports from enemy territory were entered in red in the weather charts. In the subsequent course of the war they were written in pencil and after about one day they had to be erased again.

2) Impending Allied air attacks from southern Italy on Rumania and Hungary and the expected strength of the attacking formations were recognized in good time by the German air defence by intercepting the tuning traffic of the enemy aircraft over their airfields in Southern Italy.

3) Extensive demolitions behind the enemy front were carried out in Russia and during the German withdrawal by wireless from aircraft.